DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER		
	b. SUBCONTRACT NUMBER		
X	c. SOLICITATION OR OTHER NUMBER: F04701-00-R-0202	DUE Date *(YYMMDD)*	

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	a. ORIGINAL *(Complete date in all cases)*		Date *(YYMMDD)*: 0 06 12
	b. REVISED *(Supersedes all previous specs)*	Revision No.	Date *(YYMMDD)*
	c. FINAL *(Complete Item 5 in all cases)*		Date *(YYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? [X] YES [ ] NO. If Yes, complete the following:

Classified material received or generated under F29601-97-D-0007, 8, and 9 *(Preceding Contract Number)* is transferred to this follow-on contract

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's requested dated _____, retention of the identified classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD	TBD	TBD

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD	TBD	TBD

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD	TBD	TBD

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Sounding Rocket Program
OPR: SMC/TEBI

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X	
b. RESTRICTED DATA		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X
d. FORMERLY RESTRICTED DATA		X
e. INTELLIGENCE INFORMATION		
(1) Sensitive Compartmented Information (SCI)		X
(2) Non-SCI		X
f. SPECIAL ACCESS INFORMATION		X
g. NATO INFORMATION		X
h. FOREIGN GOVERNMENT INFORMATION		X
i. LIMITED DISSEMINATION INFORMATION		X
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER *(Specify)* DOD Space System Protect Guide Information	X	

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. PERFORM SERVICES ONLY		X
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S. PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
h. REQUIRE A COMSEC ACCOUNT		X
i. HAVE TEMPEST REQUIREMENTS	X	
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
l. OTHER *(Specify)* Receive and generate Sensitive but unclassified data; and will have access to the government network	X	

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate Government authority. Proposed public releases shall be submitted for approval prior to release

[ ] Direct [X] Through *(Specify):*

See Annex 1 Attach

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review.
In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance need for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guidelines/extracts reference herein. Add additional pages as needed to provide complete*

References to the DoD Industrial Security Manual (ISM) within this form are superseded by the DoD 5220.22M, National Industrial Security Program Operating Manual (NISPOM). Other Security and Information Protect Guidance for application to this contract are attached as follows:

Annex 1, Additional DD Form 254 Guidance
Annex 2, for Official Use Only Application
Annex 3, Computer Security Measures
Annex 4, Marking, Executive Order 12958 National Security Information
Annex 5, Communication Security (COMSEC) Measures
Annex 6, Emissions Security Measures
Annex 7, Other Classification Measures

Additional required distribution: SMC/TEK, TEKB, TEBI, TEM, TEPM, FMFC

Concur,

GARY FAIN
TE Security Manager

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. *(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed)* [X] Yes [ ] No

See attached Annexes

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. *(If Yes, identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)* [X] Yes [ ] No

See Annex 1 Attached

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
JASON C. LINDGREN, Capt, USAF	Procurement Contracting Officer	(505) 853-3503

d. ADDRESS *(Include Zip Code)*	17. REQUIRED DISTRIBUTION	
SMC/TEKB 3550 Aberdeen Ave. SE Kirtland AFB, NM 87117-5776	[X]	a. CONTRACTOR
	[ ]	b. SUBCONTRACTOR
	[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE	[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	[X]	e. ADMINISTRATION CONTRACTING OFFICER
	[X]	f. OTHERS AS NECESSARY

ANNEX 1
CONTRACT NO.

DD FM 254 GUIDANCE

Remarks pertaining to Sections 10, 11, 12, 13, and 14, are as follows:

1. SECTION 10:

1.1 Contractor personnel must possess a final U.S. Government clearance at the appropriate level and be briefed (as required) for access to the below data. A list of Contractor personnel with such accesses will be provided to the SMC/TE Security Office upon request. Visit requests must identify access granted and date last briefed as appropriate. The contractor shall apply all applicable markings to the material to include warning notices. All data and materials will be handled, disclosed, transmitted, reproduced and stored in accordance with the NISPOM and organizational guidance.

Item 10a: COMSEC Information - see Annex 5 for further instructions

Item 10j: FOUO Information - see Annex 2 for further instructions

2. SECTION 11:

2.1 Item 11c:

2.1.1 All personnel assigned to this effort and handles classified information must be U.S. citizens and have a minimum of a final SECRET security clearance.

2.1.2 The contractor will require access to classified source data up to and including SECRET information in support of this work effort. Any extracts or use of such data will require the contractor to apply derivative classifications and markings consistent with the source from which the extracts were made. Refer to Annex 4, Classified Markings and Declassification Measures for further instructions.

2.1.3 See under Contract Clauses of the contract, Notification of Government Security Activity Clause, Part II. Work, to include classified automatic data processing, will be accomplished at prime contractor facilities, Kirtland AFB, Los Angeles AFB, Hill AFB, Vandenberg AFB, NASA Ranges, Space Launch Ranges, DOE Facilities and the Commercial Space Ports. When processing classified information on government furnished automated information systems (AIS) the contractor shall comply with the instructions in Annex 3, Computer Security Measures. When contractor systems are used to process classified information under this effort these instructions also apply.

2.2 Item j. Operations Security (OPSEC) is an unclassified program design to deny our adversaries access to critical information. OPSEC implementation is an inherent responsibility for all personnel that handles For Official Use Only information and other categories of sensitive information. The government has the responsibility to integrate OPSEC into plans, directives and to develop policy, provide guidance and

training. OPSEC education shall be provided to all personnel as part of in-processing and on an annual basis. General environmental awareness and proper safeguarding is the vital link to protect our critical assets. Contractors shall be required to comply with the TE OPSEC Instruction and assign program Critical Indicator Profile in performance of day-to-day duties.

2.2 Item 11l: Sensitive-but-Unclassified (SBU) automatic data processing will occur at the prime contractor facilities, Kirtland AFB, Los Angeles AFB, Hill AFB, Vandenberg AFB, NASA Ranges, Space Launch Ranges, DOE Facilities and the Commercial Space Ports. The contractor will also be granted access to networks at these locations or interface between these sites via the Internet. When processing SBU information on either government-furnished or contractor ADPE prior approval must be granted by the SMC/TE Information Protect Office. Information of an SBU nature will not be placed on the Internet without approved and tested access and security controls. This includes information that falls under the definition of Personal or Privacy Act, For Official Use Only, Scientific, Technical or Research and Development.

3. SECTION 12:

There will be no voluntary public release of information concerning this contract. Requests for public release of information concerning this contract shall be submitted through SMC/TEX, and SMC/PAS, as appropriate, 45 days in advance of scheduled release date. Answers to queries may be made only with the express approval of the SMC/PAS, 160 Skynet St, El Segundo, CA. No other dissemination of information is authorized. This prohibition extends to all publications of an informational nature both internal and external, and to all conversations except those required for conduct of official business.

4. SECTION 13:

4.1 Executive Order 12958, Classified National Security Information, contains new classification, declassification, and marking requirements which **are not** the same as those of the NISPOM. The Marking Guide at Annex 4 is provided on specific instructions while the NISPOM is being revised to incorporate these changes. Unless approved by the Contracting Officer the Contractor **does not** have to remark existing classified documents to comply with the new requirements.

4.2 Classified information may be transmitted through the Internet if encrypted utilizing National Security Agency approved encryption methods. Only releasable public information may be directly accessed from the Internet without access and/or security controls. All information maintained on a computer system connected to the Internet and not protected by access controls must be public access information. The following types of unclassified information **shall not** be placed on the Internet without approved and tested access and security controls: (a) For Official Use Only; (b) Personal or Privacy Act; (c) Scientific, Technical or Research and Development; and, (d) Unclassified information that requires special handling. Refer to Annex 2, For Official Use Only Application, for additional instructions.

4.3 Refer to Annex 7, Other Classification Measures, with regard to Security Classification Guidance and Protect Guides under this contract.

5. **SECTION 14:** Additional security requirements, in addition to the NISPOM and associated annex(es), are established. Refer to the appropriate annex to the DD Fm 254 for these requirements and guidelines.

6. **NOTE:** Changes to the DD 254 will be addressed as required to satisfy mission needs.

ANNEX 2
CONTRACT NO.

FOR OFFICIAL USE ONLY APPLICATION

1. WHAT IS THE "FOR OFFICIAL USE ONLY" MARKING?

"For Official Use Only" (FOUO) is not a classification (e.g., confidential, secret, top secret). It is a SENSITIVITY designation, intended for marking correspondence to call attention to the FOUO content and ensure its proper protection, distribution and handling. FOUO should only be disseminated to those personnel, agencies or organizations that have a need-to-know in performance of official U.S. government duties. Particular attention should be paid when information involves: (a) external DoD agencies; (b) OCONUS operations (government and contractor) such as NATO and NORAD; (c) foreign interests (e.g., joint-owned companies); and, (d) unclassified associations when in aggregation can upgrade the data to a National Security classification (e.g., SECRET).

2. WHEN TO USE "FOR OFFICIAL USE ONLY" (FOUO) ON CORRESPONDENCE OR SIMILAR MATERIALS?

Correspondence or similar materials that fall in the below categories it should be marked FOUO:

a. **Personal Data (Privacy Act).** Manpower and personnel records, medical records, individual financial records, training records, and similar personal information in other files whose release to the public clearly invades personal privacy. This includes name/address/unit and similar information of personnel serving overseas or in sensitive or routinely deployable units.

b. **Contracting related data** (e.g., evaluations of contractors and their products, Source Selection Sensitive, Procurement data)

c. **Confidential Commercial Information** (e.g., Proprietary Data)

d. **Staff Judge Advocate records** (e.g., litigation, deliberations, attorney-client communications)

e. **Civil Engineering related data** (e.g., proposals to buy, lease, or otherwise acquire and dispose of materials, real estate, facilities, or functions)

f. **Official Reports of Inspections, Audits, Investigations, or Surveys** (e.g., safety, security, or internal management, administration, or operation of the Air Force)

g. **Technical and Scientific Data** (e.g., trade secrets or other confidential research, development, or commercial information the Air Force or DoD owns; unclassified aggregated data)

h. **Planning, Programming, and Budget Information** (e.g., involving defense planning and resource allocation; financial data)

i. **Training Records** (e.g., for special activities or classified missions, intelligence training, training involvements with foreign personnel)

j. **Investigative Records** (e.g., law enforcement, violation or incident documentation, identifies a confidential source or foreign agency or authority or private institution, discloses security methodologies)

l. **Inter- and Intra-agency records** (e.g., Chaplain records; internal organizational management records; quality assurance data, credentials; safety records; logistics records; automated decision-making aids; maintenance records; critical technologies; critical indicators, vulnerabilities and countermeasures; unclassified nuclear controlled information; unit mobility or deployment information; war reserve material data; aggregated data)

m. **Internal Personnel Rules and Practices**. (1) Records, if disclosed, would substantially hinder the effective performance of a significant function of the DoD by risking circumvention of a statute or Air Force instruction or policy. (2) trivial internal administrative matters of no genuine public interest and the process of releasing such records would constitute an unwarranted administrative burden.

3. WHAT DOCUMENT AND MATERIAL TYPES SHOULD BE MARKED?

Documents, computer printouts, photographs, films, tapes, slides, diskettes, etc..

4. WHEN SHOULD CORRESPONDENCE OR SIMILAR MATERIALS BE MARKED 'FOUO'?

a - At the time of origination, whether in draft or final form.

b - When a previously CLASSIFIED document is downgraded to an UNCLASSIFIED status and contains FOUO information.

c - When specific paragraphs of a CLASSIFIED DOCUMENT contains FOUO information (and no other classified information), that paragraph may be marked FOUO to denote the highest sensitivity level applied.

d - An explanation of the FOUO marking restriction to include distribution and destruction instructions should be specified either within the first few pages of the document or the cover page.

e - Mark an unclassified document containing FOUO information "For Official Use Only" at the bottom, on the outside of the front cover (if any), on each page containing FOUO information, on the back over (if any).

f - In unclassified documents, the originator may also mark individual paragraphs that contain FOUO information to alert users, such as in cases where information is redistributed multiple times (e.g., e-mail attachments). This will also aid greatly in identifying whether certain information is releasable to the public in response to Freedom of Information Act requests.

5. HOW TO HANDLE FOUO CORRESPONDENCE OR SIMILAR MATERIALS?

a - Do not leave it laying around where it can be easily recognized or so anyone can access it. For example, turn it faced down on your desk when in temporary use. Put away in a desk drawer or file cabinet for extended periods when not in use.

b - More sensitive FOUO information should be locked in a drawer or file cabinet. FOUO information is not considered classified it MAY NOT be kept in a safe, unless part of a classified file or record.

6. WHEN CAN FOUO BE TRANSMITTED VIA NETWORKS?

a - FOUO information may be transmitted among functional areas within TE (e.g., intra-nets; TE subnet) and other on-site networks (e.g., PL net) that DO NOT require access to the INTERNET.

b - When adequate security controls are in place and approved by the Designated Approving Authority (DAA), FOUO information may be placed on the INTERNET or transmitted via other external networks.

c - Only public releasable information may be placed on the INTERNET without encryption. Information that will be made public across the Internet must be cleared through the Public Affairs channels.

7. HOW TO DESTROY FOUO CORRESPONDENCE OR SIMILAR MATERIALS?

Destruction is based upon the sensitivity of the FOUO information. The three primary methods of FOUO destruction used within TE are:

a - Destroy by any means of shredding (you DO NOT need a witness present).
b - Tearing papers up in tiny pieces so they can not be put back together and throw into trash containers.
c - Delete FOUO information from media when no longer needed (degaussing diskettes or using an overwrite routine is not mandatory).

8. WHAT IS THE STATUS OF SUPPORTING SECURITY REQUISITIONS?

Industry confidential bins may be used to store FOUO materials awaiting destruction. These bins lock to provide the level of protection necessary to store various levels of sensitive FOUO materials for destruction, and to maintain a level of control to prevent unauthorized retrieval by personnel without a need-to-know. They CAN NOT be used to store National Security classified information (e.g., CONFIDENTIAL).

ANNEX 3
CONTRACT NO.

COMPUTER SECURITY MEASURES

PART I - GENERAL REQUIREMENTS

1.0 PURPOSE AND SCOPE

1.1 This annex provides specific Computer Security (COMPUSEC) measures required for the operation of all automated information systems (AIS), including command, control, communications and computer (C4) systems and word processors, to process classified information. These measures apply to AIS platforms such as main frame systems, subsystems, desktops, and portables. The goal is to ensure AIS information protection and secure operations consistent with classification and sensitivity elements and mission requirements.

1.2 These COMPUSEC measures complement, but do not replace or supersede Air Force, DoD or other directives pertaining to AIS processing and information protection. Additionally, more detailed guidance is also contained within the contents of the DD Fm 254, Contract Security Classification Specification on FOUO data and Internet policy. Questions or concerns on this annex should be referred to the TE Information Protect Office (SMC/TEM, 3550 Aberdeen Avenue, Kirtland AFB NM 87117) for resolution. Specific references are as follows:

1.2.1 AFPD 33-2, Information Protection
1.2.2 AFI 33-202, The Computer Security Program, 1 Feb 99
1.2.2 AFSSI 5100, Security Policy Development Guide, 22 Jul 96

1.3 These measures are applicable to all Air Force owned and operated AIS and contractor systems that come under Air Force operational approval jurisdiction.

2.0 COMPUSEC CONTROLS

2.1 The SMC/TE Director is the Designated Approving Authority (DAA) responsible for approval to operate or use AIS resources under his/her jurisdiction. The SMC/TEM is the Office of Primary Responsibility for COMPUSEC management to provide overall systems security oversight and protection.

2.2 The government functional area chief is the Computer Systems Manager and will assign a Computer System Security Officer (CSSO) to interface with the TE COMPUSEC Manager and contractor affected COMPUSEC elements. The contractor appointments are required as noted below.

2.2.1 For AIS at contractor facilities, appoint in writing a System Security Officer for each major system that processes classified information or set of minor systems collocated which process either classified or unclassified information.

2.2.2 For AIS on government premises, identify in writing a Terminal Area Security Officer upon request by either the CSM or CSSO. The system administrator may serve in this role.

3.0 POLICY

3.1 Contractors who operate or use an Air Force owned and controlled AIS, whether located on or off the Air Force premises, will implement the measures described herein.

3.2 Contractor-owned or operated hardware and software used on Air Force premises or for government activities must meet all security requirements for government-owned hardware and software.

3.3 All AIS required to process classified information must receive prior approval for the highest level of classified to be processed on the system. Air Force owned and controlled AIS which process unclassified information must also receive prior approval to use or operate.

3.4 Develop and maintain the required documentation to support DAA accreditation and certification of assigned AIS, as well as, operator and user documentation.

3.5 Foreign-owned or operated AISs shall not be used to process sensitive-but-unclassified (SBU) or classified information or for critical processing, except if required by international treaties or security agreements.

3.6 Personally Owned hardware or software shall not be used to process classified information. DAA approval is mandatory for approval of personally-owned resources to process unclassified and sensitive-unclassified information.

3.7 Contractor personnel are highly encouraged to participate in government-provided awareness, training and education. The conduct of special awareness, training and education for contractor personnel will be processed through the Contracting Officer for required attendance.

3.8 Report all AIS vulnerabilities, security incidents, and virus attacks to the government Computer System Security Officer to whom reporting or where assigned. Prompt verbal notification at the time occurrence is required and a written statement within 24 hours thereafter.

4.0 RESPONSIBILITIES

4.1 ***The Air Force is responsible for:***

4.1.1 Approving all AIS which process classified information regardless of how the system was acquired.

4.1.2 Reapproving all AIS to continue processing classified information, annually or whenever the AIS is relocated, modified or the mode of operation changes.

4.1.3 Approving procedures developed by the user to implement the Operating Security Measures (i.e., declassification programs for storage media).

4.1.4 Auditing the ADP system for compliance with approved operating security measures.

4.1.5 Informing the contractor of awareness, training and education for participation.

4.1.6 Responding to incident notifications and follow through to closeout.

4.2 The contractor is responsible for:

4.2.1 Developing procedures to implement the COMPUSEC measures contained herein.

4.2.2 Ensuring all personnel working within the AIS environment receive annual training on the COMPUSEC measures contained herein.

4.2.3 Ensuring all vulnerabilities and incidents associated with an AIS are promptly reported.

4.2.4 Ensuring the SSO or TASO is on duty or call whenever an AIS processes classified information.

4.3 ***The SSO is responsible for:***

4.3.1 Ensuring that each operator has read and understand the system security operating instructions and uses them when processing classified and SBU information.

4.3.2 Reporting all suspected or actual security vulnerabilities or incidents to the proper Air Force authorities.

4.3.3 Reporting any planned or actual system, environment, procedural, etc., changes affecting the system to the CSSO for assessment of security impact.

4.3.4 Ensuring that an individual is identified to assume this security responsibility before he/she departs or otherwise is relieved from this responsibility and notifies the CSSO in wiring of any such change.

5.0 OPERATING SECURITY MEASURES

5.1 Access to/safeguarding systems processing classified information:

5.1.1 All personnel who are permitted access to the immediate equipment area or emote peripheral area of an AIS during classified session must have both the clearance and need-to-know for the information being processed at that particular time.

5.1.2 An access list of personnel who have both clearance and authorization to access the immediate equipment and during a classified processing session will be maintained. This list must be readily available to the operators for identification and authentication purposes.

5.1.3 Only authorized vendor personnel may be permitted escorted access for maintenance purposes, and they will be observed at all times by personnel who are knowledgeable of the AIS.

5.1.4 Each person who operates the system to process classified information must certify that they have read, understand, and will employ these procedures during all sessions. The SSO will also ensure that an annual review of these security procedures is accomplished by operators.

5.2 Audit Trails: The general security requirement for any AIS audit trail is to provide a documented history of the use of the system. Audit trails (manual, automated or a combination of both) must document significant events occurring in the following areas of concern:

5.2.1 When the system is declassified and by whom.

5.2.2 When and who uses the system and if classified information is processed.

5.2.3 When system is inactive and if it was declassified.

5.2.4 When system is down for maintenance who does maintenance.

5.2.5 When remote terminals are connected and when disconnected.

5.2.6 When errors occur which point toward a potential vulnerability, incident or malicious logic activity.

5.3 Classified Storage/Output Media:

5.3.1 All computer output (tapes, disks, printout, etc.) generated on a system which processes classified information will be handled/destroyed as classified of the highest level in the system; unless it has specifically been reviewed and is determined to be unclassified by a knowledgeable individual.

5.3.2 All classified printed output will, as a minimum, be marked at the top and bottom of the first and last pages with the highest level of material included in the document. Markings must standout from that of the main text. Refer to Annex 2 for marking classified materials and AIS resources.

5.3.3 All carbon paper from multiple-part paper which contains classified information will be destroyed as classified waste.

5.3.4 Printer ribbons will be marked indicating the highest level of information in the system. All printer ribbons used to print classified information will be stored in an

authorized container during unmanned periods and destroyed as classified waste when no longer serviceable.

5.3.5 Classified keypunch card decks and similar card decks will have the classification level indicated in the header of the first card and be manually stamped on the first and last card of the deck.

5.3.6 All on-line disk storage will be handled at the highest level of classified information contained on the system.

5.3.7 Removable/off-line storage media (e.g., magnetic tape, floppy disks, etc.) will be marked, handled, and stored according to the highest level of information contained on them.

5.4 Declassification of ADP Equipment and Storage Media

5.4.1 Declassify ADP equipment and storage media when changing modes of operation, changing operations to lower classification level (to prevent the unauthorized disclosure of residual classified information when left unprotected, and when no longer required.

5.4.2 To declassify Video Display Terminals (VDT) and Cathode Ray Tubes (CRT) the brightness control is varied from minimum to maximum. This will enable you to determine if any classified data is retained in the screen's phosphorus coating. If the inspection reveals classified information, the device must be retained within the appropriate security environment. If there is no classified information, the VDT/CRT may be handled as unclassified.

5.4.3 Declassification methods for electronic/magnetic storage devices are contained in Part II.

5.4.4 Declassification of printer ribbons, card decks, computer printouts, and carbon paper will be by destruction as classified waste in accordance with DoD 5200.1R.

5.5 Vendor Maintenance

5.5.1 Preventive Maintenance and Remedial Maintenance by vendors (without both clearance and need-to-know) will only be accomplished under the direct supervision of a cleared, knowledgeable "system operator/programmer" level individual. This individual will ensure that the vendor accomplishes only pre-discussed, agreed to maintenance routines.

5.5.2 On-Line Storage Media. Unless maintenance personnel have proper clearances and need-to-know, maintenance which requires access to on-line storage media will only be performed after media has been declassified.

5.5.3 Main Memory. Maintenance requiring access to main memory will only be performed after the main memory has been declassified (refer to paragraph d above).

5.5.4 Hard Disk Failures. In the event of a hard (fixed) disk failures where a declassification program cannot be used, the fixed disks must be removed by the vendor and turned over to the operator. Prior to sending the disk drive out for service, the disk drive must be degaussed. If the disk drive cannot be declassified or degaussed, the system operator must destroy the bad disk in accordance with DoD 5200.1-R and Air Force supplements to prevent compromise.

5.6 Safeguarding During Unmanned Periods:

5.6.1 AIS used to process classified information can not be left unguarded unless it is located within an approved secured and alarmed facility or has been declassified.

5.6.2 AIS will have all classified removable storage media (e.g., floppy disks) removed to prevent unauthorized access during unmanned periods. This removable storage media and all keys for systems switches will be locked within an approved safe during unmanned periods. (NOTE: Some systems require a disk cartridge be in place at all times to prevent contamination. Use an unclassified disk for this purpose.)

5.6.3 Printer ribbons used to print classified information will be labeled, removed, and stored in an approved safe during unmanned period.

5.7 Computer Fraud, Waste and Abuse: Misuse of Government AIS resources is subject to administrative or disciplinary actions. All personnel must be aware of this potential for misuse and the consequences. System programmer/operators must maintain an awareness of system usage and report abuses to management for resolution.

5.8 Malicious Logic: Ensure adequate controls are in place to prevent malicious logic (e.g., trojan horses, trap doors) to AIS resources. Ensure virus prevention software is loaded on all AIS and implemented for detection at various system operating levels.

5.9 Contingency Plans: For the protection of Government owned AIS resources, the contractor shall develop contingency plans which will address the following areas:

5.9.1 Protection or disposal of classified information/data and equipment;

5.9.2 Protection of sensitive but unclassified information/data;

5.9.3 Fire evacuation and prevention;

5.9.4 Data or file reconstruction;

5.9.5 Identification of emergency reporting;

5.9.6 Back up and off site storage;

5.9.7 Priority scheduling;

5.9.8 Bomb threats;

5.9.9 Site Evacuation; and,

5.9.10 Alternate site deployment and operation if required by the contract.

PART II - DECLASSIFICATION OF STORAGE MEDIA

1.0 DEFINITION. Declassification in this context means the effective erasure of storage media such that the extraction of residual classified information for the media either is not possible or is prohibitively difficult under separate laboratory conditions when the media are released from continuing security controls.

2.0 VERIFICATION. Results of declassification procedures shall be verified by the Air Force. This should be accomplished through a practical approach keyed to the media or equipment in question and designed to obtain reasonable assurance that the declassification action has been fully and successfully accomplished as intended. In verifying overwrite actions, for example, it is not intended that the overwrite action of each storage locations in two or more overwrite cycles is considered adequate for this purpose and maybe accomplished by readout (hard copy or visual), or through hardware and/or software verification.

3.0 DECLASSIFICATION PROCESS. Approved Air Force utility software may be used to execute certain of the below declassification functions.

3.1 Magnetic storage media:

3.1.1 Bubble memory. One overwrite.

3.1.2 Data (tape) cartridge. Approved tape degausser with appropriate adapter, as may be required.

3.1.3 Digital (tape) cassette. Approved tape degaussers with appropriate adapter, as may be required.

3.1.4 Disk cartridge. Overwrite once with binary high values (all ones), once with binary low values (all zeros) and once with any other character.

3.1.5 Disk pack.

3.1.5.1 Approved magnetic device.

3.1.5.2 Overwrite once with binary high values (all ones), once with binary low values (all zeros) and once with any other character.

3.1.6 Diskette. See Flexible Disk

3.1.7 Drum.

3.1.7.1 Approved permanent magnetic device.

3.1.7.2 Overwrite once with binary high values (all ones), once with binary low values (all zeros) and once with any other character.

ANNEX 4
CONTRACT NO.
MARKING

Furnished upon request.

ANNEX 5
CONTRACT NO.

COMMUNICATIONS SECURITY (COMSEC) MEASURES

1.0 GENERAL. The contractor shall, in addition to the requirements set forth in the DoD National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-R), and the COMSEC Annex (DoD 5220.22-A) comply with the written instructions of the installation Commander regarding communications security matters.

2.0 PURPOSE. Provides for additional security measures required by the Government to be taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications. COMSEC protection results from the application of security measures to electrical systems which generate, handle, process, or use national security information.

3.0 REFERENCE. Item 11h of the DD Fm 254

4.0 COMSEC AND/OR CRYPTOGRAPHIC ACCESS

4.1 The contractor is governed by DoD 5220.22S, COMSEC supplement to the NISPOM. Access to COMSEC material/information is restricted to U.S. citizens holding final U.S. government clearances and is not releasable to personnel holding only a reciprocal clearance. Personnel requiring COMSEC access shall be briefed in accordance with DoD 5050.22S.

4.2 The Air Force program/project manager shall designate the number of personnel requiring cryptographic access. The number will be limited to the minimum necessary and will be on a strict need-to-know basis.

4.3 The COMSEC/CRYPTO briefing applies only to the use and control of crypto equipment and specialized COMSEC publications. NACSIM/NACSEM documents are not considered COMSEC controlled material. Additionally, cryptographic information/equipment will not be retained in a contractor facility.

5.0 INTERNET POLICY AND ENCRYPTION

5.1 Classified information may be transmitted through the Internet if encrypted utilizing National Security Agency approved encryption methods. Only releasable public information may be directly accessed from the Internet without access and/or security controls. All information maintained on a computer system connected to the Internet and not protected by access controls, must be public access information.

ANNEX 6
CONTRACT NO.

EMISSIONS SECURITY (EMSEC) MEASURES

1.0 PURPOSE. Provides for additional security measures required by the Government to be taken to deny information which might be derived from the interception of compromising emanations from electronic equipment.

2.0 REFERENCES. Items 11C and 11I of the DD Fm 254

3.0 TEMPEST REQUIREMENTS:

3.1 The contractor shall ensure that compromising emanations conditions related to this contract are minimized. The contractor shall provide TEMPEST Countermeasures Assessment (TCA) information to the Contracting Officer and he/she will forward it to the Government EMSEC focal point (SMC/TEM). This information will be used by the Government EMSEC focal point to assess the contractor's facility. A contractor's standard security plan is unacceptable as a "stand-alone" facility information document. EMSEC requirements also apply to subcontractors; however, they should not be imposed without prior approval of the Government Contracting Office. When imposed, TCA information on the subcontractor must be submitted through the prime contractor to the Government Contracting Office. The TCA will be performed by the Government TEMPEST authority using current Air Force EMSEC directives.

3.2 The contractor should not expend any resource other than providing the TCA information until the TEMPEST assessment is completed and direction is provided through the contracting officer. TEMPEST is applied on case-by-case basis and further information may be required to complete the TCA; should this be the case, the contractor will provide this information to the Contracting Officer when requested. During the facility assessment period, contractors should reply to questions with specific and timely answers.

3.3 Equipment used by the contractor to process SECRET information must at a minimum meet the TEMPEST Red/Black separation requirement listed on the attached sheet. Based on the results of the TCA additional requirements may be imposed.

3.4 The contractor must submit to the Program Management Office (SMC/TEOT) an Equipment Change Notification (ECN) to advise the PMO of any proposed change or relocation of equipment used to process SECRET (or higher) information. The ECN must be submitted at least 30 days before the change or relocation occurs.

3.5 The contractor must submit to the PMO a new TCA at least 30 days before processing SECRET or higher information in a different facility than that specified in the original TCA.

3.6 Classified processing shall not commence until the TCA has been evaluated and approved by the Government TEMPEST authority, and the Automated Data Products (ADP) procedures have been approved by the Cognizant Security Office. The contractor will then be notified by the contracting officer that classified processing can begin.

4.0 TEMPEST COUNTERMEASURES ASSESSMENT INFORMATION FORMAT

(See above paragraph)

4.1 System Description Data:

4.1.1 System/Facility: Provide full name and address of company submitting request and RFP/contract number and duration. Provide names and addresses of additional facilities and subcontractors, if any, that will process SECRET or higher information in support of this contract. A separate TCA must be performed by the Government TEMPEST authority for each facility that will process SECRET or higher information. Also provide a brief title identifying the overall system or facility (i.e., test launch facility, command post word processing system, plans and programs interactive graphics, system, etc.).

4.1.2 Location: Identify the address (including city, state, facility, building and room number) where the system and facility are located. Facility diagrams (outer perimeter) and floor plans for each floor and room that will be processing classified information must be submitted.

4.1.3 Equipment: List the manufacturer and exact model number, nomenclature (terminal, disk drive, video systems, etc.) and quantity of each piece of equipment involved in classified processing.

4.2 Responsible Personnel. Provide Security Officer/Manager and System Custodian point of contact name, title, office symbol and phone number for each facility. Include the Company Appointed TEMPEST Authority (CATA) if there is one.

4.3 Operational Risk: Estimate the percent of total material processed for each level of classification. Estimate the volume on a per day basis by bytes, lines, pages or hours for each classification. If the same equipment will be used for classified processing in support of other projects, list classification(s) and percentage(s) of use by other programs.

4.3.1 Physical Security: Provide information on security procedures for control of personnel gaining access to the buildings and rooms (i.e., key card access, security desk, cipher lock access, etc.) where classified processing will be done.

4.3.2 Give brief description of building (brick, wooden, windows, number of floors, loading docks, etc.).

4.4 Remarks. Provide any amplifying information that could assist in determining the hazard and risk situation for the facility in question.

5.0 TEMPEST SEPARATION REQUIREMENTS

5.1 Countermeasures Application. These paragraphs discuss how to apply the countermeasures and under what conditions they would not be required.

5.1.1 Keep RED and BLACK signal lines separated. Keeping RED signal lines about six inches away from BLACK signal lines will reduce coupling to a level low enough to prevent detection at great distances (over one mile). This separation may be reduced to two inches if the RED signal lines are shielded.

5.1.2 Keep RED signal lines separated from BLACK Power lines. Keeping RED signal lines about six inches away from BLACK power lines will reduce coupling to a low enough level to prevent detection at great distances (over one mile). This separation may be reduced to two inches if the RED signal lines are shielded.

5.1.3 Keep RED processors separated from BLACK telephones and telephone lines. Keep non-TEMPEST-approved printers at least six feet away from telephones. Do not use the telephone while printing classified information. Keep all non-TEMPEST-approved equipment at least three feet away from the telephone lines; two inches if the telephone lines are shielded.

6.0 TEMPEST SEPARATION MATRIX

RED/BLACK	CRYPTO EQUIPMENT	UNSHIELDED SIGNAL AND TELEPHONE LINES	SHIELDED TELEPHONE LINES	POWER LINES
Crypto Equipment	0000	3ft	2in	2in
Unshielded Signal Lines	6in	6in	3in	6in
Shielded Signal Lines	2in	2in	2in	2in
TEMPEST-Approved Equipment	2in	6in	2in	NONE
Non-TEMPEST-Approved Equipment	3ft	3ft	2in	NONE

ANNEX 7
CONTRACT NO.
OTHER CLASSIFICATION MEASURES

1.0 SECURITY CLASSIFICATION GUIDES

Security Classification Guides (SCG) to include any changes or revisions will be made available to the contractor in performance of contractual tasks as required.

2.0 PROTECT GUIDES

The DoD Space Systems Protect Program, DoDD 3500.2 dated 1 Oct 96, implements the National Security Policy and DoD Space Policy and requires RDT&E entities develop protect guides for major systems and support capabilities. This is an effort to reduce the number of SCGs and focus information classification at the system level. Protect guides are also developed for modernization and development, test and operations purposes. Applicable SCG content will be considered when developing protect guides for SMC/TE.

3.0 ORIGINAL CLASSIFICATION AUTHORITY (OCA) AND DECLASSIFICATION AND DOWNGRADING AUTHORITY (DDA)

3.1 Delegation and Authorization. The Secretary of the Air Force is responsible to make appointments and delegations, in accordance with Executive Order 12958, of those Air Force positions authorized to originally classify and declassify or downgrade classified information and their level of authority. For example, only an OCA can classify information at the level authorized, and only a DDA can authorize declassification or downgrading of that information. The contractor's classification of information is derivative to the original guidance, and actions to declassify or downgrade this information should be in accordance with DDA guidance. This guidance is generally provided in the form of an SCG but may also be provided by other written medium.

3.2 Classification Challenges. Requests to challenge information classification, or to have information declassified or downgraded outside of its specified time, should be submitted through the SMC/TE Security Office for OCA and DDA action. Pending an OCA or DDA reply the classified information will be handled at its current level of classification.